Published on *The National Law Review* https://natlawreview.com

Bridging the Week by Gary DeWaal: August 13 to 17 and August 20, 2018 (ICO Halted; Misappropriation of Client Funds Not Halted; Rogue Trading)

Article By:

Gary De Waal

The Securities and Exchange Commission banned the founder of a company that it claimed was involved in an illicit initial coin offering of a new digital token from ever serving as an officer or a director of a publicly-traded or reporting company. Importantly, although this action involved an ICO, the relevant digital token was not associated with any proposed new application on any blockchain. The SEC also fined a combined investment adviser and broker-dealer for not having written policies and procedures designed to detect misappropriation of customer assets by rogue representatives. And, unfortunately, misappropriation occurred. As a result, the following matters are covered in this week's edition of *Bridging the Week*:

- Company Founder Banned by SEC for Allegedly Fraudulent and Unregistered ICO (includes **Legal Weeds**);
- Investment Adviser Sanctioned US $4.5 Million for Not Having Policies Reasonably Designed to Protect Investor Assets Against Misappropriation (includes **Compliance Weeds**); and more.

Article Version:

Briefly:

- **Company Founder Banned by SEC for Allegedly Fraudulent and Unregistered ICO**: In response to an enforcement action by the Securities and Exchange Commission, David Laurance consented to a permanent prohibition from acting as an officer or director of a publicly traded or reporting company, as well from being associated with any offering of a penny stock company, because of his purported involvement in the illicit offering of digital tokens known as "Tomahawkcoins" ("TOM") from July through September 2017. Mr. Laurance allegedly engaged in such offering in conjunction with Tomahawk Exploration LLC, a company of which he was the founder and sole managing director.

According to the SEC, during the relevant time, the respondents sought to raise US $5 million through an initial coin offering of TOMs to support an oil and gas exploration project. Potential purchasers of TOMs were told they could trade their digital tokens on a token trading platform for potential profits and would have an option to convert their TOMs into Tomahawk equity at a later time.

TOMs were marketed as "low risk" with high potential rates of return, said the SEC. Moreover, the SEC noted that Tomahawk claimed that its "risk-adjusted returns are exceptional," and implied it had a lease for oil drilling when it did not. The SEC charged that these and other promotional statements were materially false and misleading. Additionally, Tomahawk's website pronounced that the company's principals were "successful citizens with flawless backgrounds" when, in fact, Mr. Laurance was convicted in 1993 of mail fraud and for providing false information to the SEC in connection with a penny stock scheme he promoted and controlled.

Apparently, the respondents did not raise any funds through their ICO. However, said the SEC, Tomahawk issued 80,000 TOMs to persons in exchange for online marketing and promotional services as part of a so-called “Bounty Program.” Recipients of TOMs were able to convert their digital tokens to other crypto assets on a decentralized platform.

The SEC claimed that the Bounty Program constituted the offer and sale of securities that were required to be registered (or issued pursuant to a bona fide exemption) but were not.

In addition to his agreement to an officer, director and penny stock bar, Mr. Laurance agreed to pay a fine of US $30,000 spread out over 1020 days, and both respondents consented to a cease and desist order. (The payment schedule appears to reflect the SEC's acknowledgement of Mr. Laurance's poor financial condition.) The respondents did not admit or deny any of the findings by the SEC with limited exception.

Separately, a federal court in Brooklyn, New York held that two non-United States based individual defendants and an unincorporated entity they controlled – PlexCorps – had sufficient contacts with the US to sustain the court’s personal jurisdiction over them in connection with in an SEC enforcement action against them related to another purported fraudulent ICO.

Last year, the SEC obtained an emergency asset freeze from the court to halt the ICO which involved PlexCoin digital tokens that began in August 2017. According to the SEC, the ICO – which was orchestrated by Dominic Lacroix and Sabrina Paradis-Royer of Quebec, Canada, through PlexCorps – was marketed as a means for investors to obtain a new “tokenized currency” that would net early purchasers a very high rate of return. These returns would supposedly derive from the appreciation in value that would result from investments PlexCorps would make with the ICO’s proceeds; proceeds distributed to investors from PlexCorps’ profits; and the appreciation in value of PlexCoins when traded on digital asset exchanges.However, charged the SEC, the defendants’ offering was fraudulent and the proceeds of the ICO were never to be used for legitimate business development. (Click here for further background in the article “SEC Obtains Emergency Asset Freeze to Stop Purportedly Fraudulent Initial Coin Offering” in the December 10, 2017 edition of *Bridging the Week*.)

The individual defendants subsequently challenged the court’s personal jurisdiction over them. The court, however, denied this challenge claiming that the individual defendants had sufficient contacts with the US in connection with their purported fraudulent activity. These contacts included doing relevant business while physically traveling in the US, using US-based payment services, and marketing their products to US persons using the Internet.

The individual defendants also sought to have dismissed PlexCorps for lack of personal jurisdiction too. However, the court said the defendants offered no legal authority for their counsel to make this motion and therefore denied it.

Legal Weeds: Although respondents in the Tomahawk case used digital tokens and an ICO to commit their purported wrongdoing, in the end, this case apparently involved a plain vanilla unregistered stock offering fraud. The TOMs were simply used as a vogue new medium to raise funds. There was no association between TOMs and any proposed new blockchain application and not any attempt by respondents to market TOMs as utility tokens. As I was quoted in the *NY Post* this week, “This is just another wolf in a different type of sheep’s clothing, but it’s still sheep’s clothing” – let alone, ultimately, a wolf! (Click here for access to the relevant *NY Post* August 14, 2018 article.)

(Typically, the term “utility token” references a digital token that has express functionality authorizing a holder to access or purchase assets based on a specific blockchain technology.)

The SEC has cautioned that digital tokens issued through ICOs to raise funds may be securities,

even if the expectation of profits to purchasers is solely through secondary market trading. This would be the case even if such tokens might be labeled as utility tokens. (Click here for background in the article “Non-Registered Cryptocurrency Based on Munchee Food App Fails to Satisfy SEC’s Appetite for Non-Security” in the December 17, 2017 edition of *Bridging the Week*.) Since issuance of its DAO report in July 2017, officers of the SEC have generally voiced the opinion the most if not all ICO-issued tokens are likely investment contracts and thus securities. (Click here for an example, in the article “SEC Chairman Warns Lawyers Providing “It Depends” Advice on ICOs” in the January 28, 2018 edition of *Bridging the Week*.)

Recently, William Hinman, Director of the SEC’s Division of Corporate Finance indicated that he could envision that certain utility tokens might not always be securities. He said that such a conclusion might be appropriate “where there is no longer any central enterprise being invested in or where the digital asset is sold only to be used to purchase a good or service available through the network on which it was created.” (Click here for background in the article “Anything but Sleep Inducing: SEC Corporate Finance Director Says Ether Not a Security and Canada Issues Guidance on Utility Tokens” in the June 17, 2018 edition of *Bridging the Week*.)

In July 2018, the Token Alliance – an industry initiative of the Chamber of Digital Commerce – issued a comprehensive overview of the regulation of digital assets in the US and other select jurisdictions, and proposed best practices for sponsors of digital tokens that are not intended to be securities or an instrument over which the Commodity Futures Trading Commission might have anti-fraud or anti-manipulation authority – i.e., utility tokens. (Click here for details in the sub-article "Token Alliance's Best Practices for Non-Securities Utility Tokens" in the August 5, 2018 edition of *Bridging the Week*.)

- **Investment Adviser Sanctioned US $4.5 Million for Not Having Policies Reasonably Designed to Protect Investor Assets Against Misappropriation**: Ameriprise Financial Services, Inc., a registered investment adviser and broker-dealer, agreed to pay a fine of US $4.5 million to resolve allegations made by the Securities and Exchange Commission that, from 2011 through 2014, it failed to have and follow adequate written policies and procedures designed to prevent the misappropriation of client assets by persons associated with the firm.

The SEC said that, during the relevant time, five firm representatives engaged in various fraudulent acts, including forging customer documents, to steal over US $1 million of customer funds. Although Ameriprise considered fraud by its employees to be a risk for which it implemented an express compliance and supervisory framework that relied on various manual and automated tools, aspects of two of its automated tools to detect fraud and misappropriation broke down and contributed to the relevant fraud not being caught, claimed the SEC.

In one circumstance, a program meant to detect when an account address was changed to an address of a person associated with Ameriprise failed to work properly and was not tested until December 2013. As a result, in part, said the SEC, two representatives were able to change addresses for two of their clients to their home addresses, thus facilitating fraudulent check disbursements.

In the other circumstance, a program intended to detect suspicious disbursements made by check where the address of a payee matched the name or address of a person associated with Ameriprise was defective because the tool was too literal and solely flagged exact matches. As a result, for example, the system would not flag as suspicious a payment to an address that included “Ave.” when the address of the firm-associated person expressly included “Avenue.” The system also did not flag suspicious wire transfers. These limitations, in part, claimed the SEC, enabled the

misappropriation of customer funds by a third Ameriprise representative.

Various manual and system breakdowns also contributed to the misappropriation by the other two representatives, alleged the SEC.

In determining the amount of Ameriprise's fine, the SEC said it considered that the firm reimbursed all its customers for the misappropriated funds; fully cooperated with the Commission's investigation; retained a compliance consultant to assess the effectiveness of its policies and procedures to safeguard customer assets; and enhanced its policies and procedures, including implementing a new automated money movement and control system.

In September 2016, Ameriprise agreed to pay a fine of US $850,000 to the Financial Industry Regulatory Authority for its alleged failure to detect the conversion of US $370,000 by an office manager from five accounts of the individual's family members from October 2011 through September 2013. (Click here for details in the article, "FINRA Fines Broker-Dealer US $850,000 for Ignoring Red Flags of Office Manager's Theft of Client Funds" in the September 18, 2016 edition of *Bridging the Week*.)

Compliance Weeds: Automated surveillance systems of every kind should not just be installed and left to function on their own. Periodic testing is likely critical to assess breakdowns in expected functionality and to assess the continued effectiveness of a system in light of evolving circumstances. Testing may be particularly warranted after periodic updates or other changes to source code.

Recently, Raymond James Financial Services, Inc., a registered broker-dealer, agreed to pay a fine of US $2 million to the Financial Industry Regulatory Authority for purportedly not maintaining an adequate system to review emails by its registered representatives. According to FINRA, the firm—which relied on a surveillance system that automatically identified emails containing certain preprogrammed words—did not choose words or phrases that would identify potentially problematic conduct in light of the nature of the firm's business and prior disciplinary action taken against firm employees. Although the firm added and subtracted words over time, FINRA claimed it did so principally to reduce the volume of false positives rather than to ensure it captured all relevant emails. (Click here for additional background in the article "FINRA Fines One Broker-Dealer US $2 Million for Flawed Email Review System, and Another Broker-Dealer US $2.8 Million for Inadequate Segregation of Customer Securities" in the January 7, 2018 edition of *Bridging the Week*.)

In 2007, FINRA issued helpful guidance regarding the review and supervision of electronic communications (click here). Although intended for FINRA members, the guidance has useful information for all SEC and Commodity Futures Trading Commission-registered entities. In assessing the effectiveness of any lexicon-based automated review system, FINRA recommended that a system include a "meaningful" list of phrases and/or words (including industry jargon) based on the size of the firm, its type of business, its customer base and its location. FINRA suggested that this might necessitate inclusion of foreign language components. Overall, said FINRA, "[t]he lexicon system should be comprehensive enough to yield a meaningful sample of 'flagged' communications." Any system should have the ability to add and delete words or phrases over time, and existing words or phrases should be periodically reviewed for effectiveness.

More Briefly:

- **Bank and Broker-Dealer Affiliate Agree to US $5.75 Fine Million for Rogue Trading by Three Traders**: Citigroup Global Markets Inc. and Citigroup Inc. agreed to pay a fine of US $5.75 million to the Securities and Exchange Commission in connection with the separate, unauthorized trading by three CGMI employees of different trading desks from mid-2013 through early 2016. According to the SEC, all instances involved mismarking of "opaque,

illiquid positions that were overvalued by traders and not effectively price verified by Citi's valuation control group." The mismarking allegedly occurred over multiple quarters The SEC charged that CGMI – an SEC-registered broker-dealer and investment adviser – failed to have written policies and procedures and supervision reasonably designed to detect its traders' rogue actions earlier and that, because of the unauthorized trading, CGMI and Citigroup each sustained losses that were initially not properly reflected on their books and records.

- **Joint Audit Committee Issues Guidance Related to FCM Withdrawal of Residual Interests**: The Joint Audit Committee issued guidance to futures commission merchants regarding the withdrawal of residual interest after 12 noon. Under applicable CFTC rule, FCMs must maintain a targeted minimum amount of their own funds in each customer segregated funds category (e.g., segregated funds, secured funds and cleared swap funds) in excess of actual requirements – its so-called "residual interest." If an FCM fails to maintain funds in excess of such a level, it must immediately report the failure to the Commodity Futures Trading Commission. Each day, an FCM may only withdraw residual interest (other than for customer) after it completes and submits to the CFTC and the firm's designated self-regulatory organization its daily segregation funds calculation (by no later than noon). The JAC's guidance notes that a firm's withdrawal of residual interest after this time still may not cause the firm's excess to fall below its targeted level and sets forth criteria how an FCM might help ensure this. Among other things, the FCM must consider estimated material increases to debits and deficits as a result of top day market movements and trading activity as well as other matters that may materially impact its calculations such as investment losses or operational errors.
- **FINRA Reminds ATS System Operators of Their Supervision Duty**: The Financial Industry Regulatory Authority issued a notice reminding alternative trading systems of their obligation to monitor activity on their platforms that may violate law. This is consistent, said FINRA, with the obligation of all broker-dealers to maintain policies and procedures reasonably designed to achieve compliance with applicable laws and rules. Among other things, FINRA indicated it expects an ATS's supervisory system to be designed to act on red flags of potentially manipulative or non-bona fide trading activity. An ATS is a registered broker-dealer-operated non-exchange venue that matches buyers and sellers of securities.
- **CME Group Hits Traders for Disruptive Trading**: Members of two CME Group exchanges agreed to pay fines to settle disciplinary actions charging disruptive trading. In one matter, Joseph Gibbons agreed to pay a fine of US $15,000 and not have access to any CME Group exchange for 20 business days for entering orders during pre-open periods that were purportedly not entered in good faith. According to the relevant business conduct committee, the entry and cancellation of Mr. Gibbons's orders caused fluctuations in the displayed indicative opening price of the relevant futures contracts. In the other action, Brian Horvath agreed to pay a fine of US $15,000 and disgorge profits of US $13,275 for executing multiple user-defined spreads in order to avoid the allocation of futures contracts that should have been associated with the relevant covered options instrument. He achieved a profit equal to the amount he was required to disgorge as a result of his action.

National Law Review, Volume VIII, Number 232